

1 SHOOK, HARDY & BACON LLP
2 B. Trent Webb, Esq. (*pro hac vice*)
Peter Strand, Esq. (*pro hac vice*)
3 Ryan D. Dykal, Esq. (*pro hac vice*)
2555 Grand Boulevard
Kansas City, MO 64108-2613
4 Telephone: (816) 474-6550
Facsimile: (816) 421-5547
bwebb@shb.com

5 Robert H. Reckers, Esq. (*pro hac vice*)
6 600 Travis Street, Suite 1600
Houston, TX 77002
7 Telephone: (713) 227-8008
Facsimile: (713) 227-9508
rreckers@shb.com

8 GIBSON, DUNN & CRUTCHER LLP
9 Mark A. Perry (*pro hac vice*)
10 1050 Connecticut Avenue, N.W.
Washington, DC 20036-5306
11 Telephone: (202) 955-8500
mperry@gibsondunn.com

12 Blaine H. Evanson (*pro hac vice*)
13 Joseph A. Gorman (*pro hac vice*)
333 South Grand Avenue
14 Los Angeles, CA 90071
Telephone: (213) 229-7228
bevanson@gibsondunn.com

16 *Attorneys for Defendants Rimini Street, Inc. and Seth Ravin*

17 **UNITED STATES DISTRICT COURT**
18 **DISTRICT OF NEVADA**

19 ORACLE USA, INC., a Colorado corporation;
20 ORACLE AMERICA, INC., a Delaware
corporation; and ORACLE INTERNATIONAL
21 CORPORATION, a California corporation,

22 Plaintiffs,

23 v.

24 RIMINI STREET, INC., a Nevada corporation,
and SETH RAVIN, an individual,

25 Defendants.

LEWIS ROCA ROTHGERBER LLP
W. West Allen (Nevada Bar No. 5566)
3993 Howard Hughes Parkway, Suite 600
Las Vegas, NV 89169
Telephone: (702) 949-8200
wallen@irrlaw.com

RIMINI STREET, INC.
Daniel B. Winslow (*pro hac vice*)
6601 Koll Center Parkway, Suite 300
Pleasanton, CA 94566
Telephone: (925) 264-7736
dwinslow@riministreet.com

John P. Reilly (*pro hac vice*)
3993 Howard Hughes Parkway, Suite 500
Las Vegas, NV 89169
Telephone: (336) 908-6961
jreilly@riministreet.com

Case No. 2:10-cv-0106-LRH-PAL

**DEFENDANTS RIMINI STREET, INC.'S
AND SETH RAVIN'S REPLY IN
SUPPORT OF RULE 50(b) RENEWED
MOTION FOR JUDGMENT AS A
MATTER OF LAW**

Judge: Hon. Larry R. Hicks

TABLE OF CONTENTS

	<u>Page</u>	
I.	INTRODUCTION	1
II.	ARGUMENT	2
A.	Oracle’s Computer Hacking Claims Fail as a Matter of Law	2
1.	Rimini’s Conduct Is Not Prohibited by the Anti-Hacking Statutes	2
2.	The Statutory Provisions, Particularly as Oracle Seeks to Apply Them, Are Unconstitutional	9
3.	The State Law Hacking Claims Fail for Additional Reasons	12
B.	Lost Profits Are Unavailable for Oracle’s State Law Hacking Claims	14
1.	Lost Profits Are Not Recoverable Under the Statutes	14
2.	There Is No Evidence Supporting an Award of Lost Profits	16
C.	Oracle Concedes Judgment Is Warranted on Its Other Claims.....	18
III.	CONCLUSION	18

TABLE OF AUTHORITIES

Page(s)

Cases

4	<i>Abramson v. Brownstein,</i> 897 F.2d 389 (9th Cir. 1990).....	14
5	<i>Capitol Audio Access, Inc. v. Umemoto,</i> 980 F. Supp. 2d 1154 (E.D. Cal. 2013).....	15
6	<i>Craigslist Inc. v. 3Taps Inc.,</i> 964 F. Supp. 2d 1178 (N.D. Cal. 2013)	11
7	<i>Creative Computing v. Getloaded.com LLC,</i> 386 F.3d 930 (9th Cir. 2004).....	16
8	<i>E.E.O.C. v. Go Daddy Software, Inc.,</i> 581 F.3d 951 (9th Cir. 2009).....	14
9	<i>Elec. Funds Solutions v. Murphy,</i> 134 Cal. App. 4th 1161 (2005)	15
10	<i>Farmers Ins. Exchange v. Steele Ins. Agency, Inc.,</i> 2013 U.S. Dist. LEXIS 104606 (E.D. Cal. July 25, 2013)	15
11	<i>Ferdie Sievers & Lake Tahoe Land Co. v. Diversified Mortg. Inv.,</i> 95 Nev. 811 (1979)	13, 14
12	<i>Freund v. Nycomed Amersham,</i> 347 F.3d 752 (9th Cir. 2003).....	14
13	<i>GMC v. Eighth Judicial Dist. Court of Nev.,</i> 122 Nev. 466 (2006)	14
14	<i>Gravquick A/S v. Trimble Navigation Int'l,</i> 323 F.3d 1219 (9th Cir. 2003).....	14
15	<i>Healy v. Beer Institute,</i> 491 U.S. 324 (1989)	14
16	<i>Joseph Oat Holdings, Inc. v. RCM Digesters, Inc.,</i> 409 F. App'x 498 (3d Cir. 2010)	7
17	<i>LVRC Holdings LLC v. Brekka,</i> 581 F.3d 1127 (9th Cir. 2009).....	6, 9, 15
18	<i>Murphy v. City of Long Beach,</i> 914 F.2d 183 (9th Cir. 1990).....	14

1 **TABLE OF AUTHORITIES**
 2 (continued)

	<u>Page(s)</u>
<i>People v. Hawkins,</i> 98 Cal. App. 4th 1428 (2002)	11, 12
<i>Sanchez-Corea v. Bank of America,</i> 38 Cal. 3d 891 (1985)	15
<i>Sullivan v. Oracle Corp.,</i> 51 Cal. 4th 1191 (2011)	14
<i>United States v. Boeing Co.,</i> 9 F.3d 743 (9th Cir. 1993).....	12
<i>United States v. Christensen,</i> 801 F.3d 970 (9th Cir. 2015).....	4, 5
<i>United States v. Drew,</i> 259 F.R.D. 449 (C.D. Cal. 2009)	10, 11, 12, 15
<i>United States v. Nosal,</i> 676 F.3d 854 (9th Cir. 2012).....	1, 5, 6, 8, 9, 10, 11
<i>United States v. Valle,</i> 807 F.3d 508 (2d Cir. 2015).....	1, 8, 9, 10
<i>WEC Carolina Energy Solutions LLC v. Miller,</i> 687 F.3d 199 (4th Cir. 2012).....	8, 9, 10
Statutes	
18 U.S.C. § 1030(e)(1).....	15
18 U.S.C. § 1030(g)	15
Cal. Penal Code § 502	5
Cal. Penal Code § 502(c)	7
Cal. Penal Code § 502(c)(2).....	3, 4
Cal. Penal Code § 502(c)(3).....	4
Cal. Penal Code § 502(e)(1).....	13
Nev. Rev. Stat. § 205.511	15
Nev. Rev. Stat. § 205.4759	15

1 **TABLE OF AUTHORITIES**
2 (continued)

	<u>Page(s)</u>
3 Nev. Rev. Stat. § 205.4765	7
4 Nev. Rev. Stat. § 205.4765(1).....	4
5 Nev. Rev. Stat. § 205.4765(3).....	4

I. INTRODUCTION

Rimini Street, Inc. and Mr. Ravin (collectively, “Rimini”) are entitled to judgment as a matter of law on the state law computer hacking claims because violating a website term of use is not criminal computer hacking. The text of the statutes, binding Ninth Circuit precedent, and constitutional principles all require rejection of the jury’s verdicts—as to both liability and remedy—on Oracle’s claims under both the California and the Nevada anti-hacking statutes.

Oracle’s own witness defined hacking as “break[ing] into systems,” “penetrat[ing] through firewalls,” “exploit[ing]” “vulnerabilities in the software,” and sending “poison email messages that set up relay stations that let them get into your networks” to “make money” and “get sensitive company information and use it for financial gain.” 9/23 Tr. 1551:1-6, 1552:1-19, 1557:15-1558:6 (Screven). Rimini engaged in no such conduct. On the contrary, and critically, Oracle does not dispute that: (i) Oracle’s customers *had permission* to access Oracle’s website; (ii) Oracle’s customers *legally gave Rimini permission* to access Oracle’s website on their behalf; (iii) Rimini *acted with that permission* to download files that its clients were entitled to; and (iv) it was *lawful* for Rimini to act on behalf of its clients to download those files. Oracle does not dispute that if Rimini employees had downloaded each file individually, the hacking statutes would have no applicability whatsoever. *E.g.*, 9/17 Tr. 724:4-725:11. Oracle complains *only* that Rimini used an automated software program rather than human beings to do exactly the same thing. By unilaterally changing its terms of use to prohibit the use of such automated tools, Oracle contends, it turned Rimini’s lawful activity into a criminal violation. That is nonsensical and carries dangerous implications.

The anti-hacking statutes say *nothing* about the *means* of downloading data from a computer that a user is authorized to access. And in the controlling case of *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc), the court expressly rejected liability under the federal anti-hacking statute based solely on the fact that the conduct violates terms of use. To hold otherwise, the court reasoned, would criminalize routine private and commercial transactions, and vest the power to legislate criminal law in the hands of third parties, which would be patently unconstitutional. The Second Circuit agreed with *Nosal* in December, refusing to construe the federal anti-hacking statute to “criminaliz[e] ordinary behavior.” *United States v. Valle*, 807 F.3d 508, 528 (2d Cir. 2015).

1 Oracle's suggestion that Rimini can be held liable under state anti-hacking statutes for just such
 2 behavior cannot be reconciled with these authorities.

3 Even if hacking liability could be sustained here, the jury's damages award of \$14.4 million in
 4 "lost profits" would have to be vacated. Oracle admits that the \$14.4 million number is based on
 5 *copyright infringement* lost profits, yet (i) Oracle has identified no basis in the statutes for such an
 6 award, (ii) no court has ever awarded such damages for violations of these statutes, and (iii) courts
 7 have expressly *rejected* such damages under the analogous federal statute. In addition, there is not a
 8 shred of evidence *here* that a single customer left Oracle because of computer hacking, and \$14.4
 9 million of the damages award must be vacated on that basis as well. Oracle may recover, at most, the
 10 \$27,000 in actual costs it incurred responding to Rimini's automated downloads.

11 It is also undisputed that Oracle's remaining state law claims fail as a matter of law.

12 II. ARGUMENT

13 Neither the California nor the Nevada statute imposes liability for use of automated
 14 downloading tools, even if such tools are prohibited by website terms of use. If the statutes *were*
 15 construed to make Rimini's conduct unlawful, then they would be unconstitutional because otherwise
 16 they would render millions of daily transactions criminal conduct. Additionally, lost profits are not
 17 available under either statute and are unsupported by the evidence presented at trial.

18 A. Oracle's Computer Hacking Claims Fail as a Matter of Law

19 Judgment is warranted under both California and Nevada law because Rimini *acted with its*
 20 *clients' legal permission* when it accessed Oracle's website and downloaded support files.¹

21 1. Rimini's Conduct Is Not Prohibited by the Anti-Hacking Statutes

22 Rimini did not violate either California or Nevada's anti-hacking laws as a matter of law
 23 based on application of the undisputed facts, the plain language of the statutes, Ninth Circuit
 24 precedent, the rule of lenity, the canon of constitutional avoidance, and principles of common law.

25 ¹ Oracle now admits that the Nevada anti-hacking statute has no application. According to Oracle,
 26 "a California choice-of-law agreement controls," and a choice-of-law analysis "would lead to
 27 application of California law." Opp. at 12. Rimini continues to assert that Oracle's claims fail on
 28 the merits, regardless of which state's law applies, and regardless of the accuracy of Oracle's
 choice-of-law analysis. Nonetheless, Oracle's election constitutes an admission that judgment
 should be granted as a matter of law on the Nevada state law claim.

1 **a. Rimini Had Its Clients' Permission to Download Oracle's Materials**

2 Rimini undisputedly had permission to access Oracle's database to download support
 3 materials for Rimini's clients. Oracle does not dispute, for example, that its customers were allowed
 4 to "have consultants access the [Oracle] website on their behalf." 9/18 Tr. 866:9-12 (Allison); *see*
 5 9/22 Tr. 1201:10-13 (Renshaw) (same). Nor does Oracle dispute that the customers at issue legally
 6 authorized Rimini to access the website and download materials on their behalf. *E.g.*, PTX 482 at 3
 7 ("Our access has been approved by each of our clients").

8 The trial record further demonstrates that Rimini *did not exceed* the scope of that
 9 authorization. Rather, Rimini downloaded materials that each client was authorized to download.
 10 *E.g.*, 9/16 Tr. 281:23-282:6, 430:9-18; 9/17 Tr. 555:25-556:10, 562:21-25, 567:15-21, 728:20-22; *see*
 11 Opp. at 3 (Rimini "download[ed] these materials for clients before their maintenance contracts with
 12 Oracle expired"). Oracle disputes this fact as to only *one* client—XO. Opp. at 4, 20. But the
 13 testimony of Mr. Baron, the only evidence on which Oracle relies, confirms that Rimini's policy was
 14 to download only those materials that its clients were authorized to download. As Mr. Baron
 15 explained, if any extra content was downloaded for XO, it was because "the My Oracle website was
 16 not indexed," and, to prevent the use of any content without authorization, Rimini "downloaded by
 17 doc ID range and then deleted any content that was inappropriate for that particular client." 9/22 Tr.
 18 1234:4-17; PTX46 at 5 ("I then 'prune' this directory structure and delete directories (categories) not
 19 applicable to XO").

20 Oracle's irrelevant response is that "Defendants do not dispute that they took a great deal of
 21 data." Opp. at 21. But the statute does not prohibit taking any particular *amount* of data; the question
 22 is whether data was taken "without permission." Cal. Penal Code § 502(c)(2). Oracle does not
 23 contend in its opposition (nor did it contend at trial) that Rimini violated the statute because it "took"
 24 data without permission. To the contrary, Rimini undisputedly had permission to obtain support
 25 materials for its clients.²

27 ² Oracle also states that Rimini does "not seriously dispute that [it] 'used computer services.'" Opp. at 21. Again, Rimini *had permission* to use Oracle's database. And again, Oracle's dispute
 28 is the *means* in which Rimini used the services, not whether Rimini had permission.

1 **b. The Use of Automated Downloading Tools Is Not Computer Hacking**

2 Oracle's argument is that once it changed its website terms of use to prohibit automated
 3 downloading on February 19, 2007, the very same conduct that was lawful the day before became
 4 unlawful computer hacking, punishable as a criminal offense, the day after. This theory of liability, if
 5 accepted by the Court, would turn millions of commonplace private and commercial transactions into
 6 criminal behavior. This Court should reject it.

7 **(i) The statutes do not prohibit automated downloading**

8 Oracle does not ground its arguments in the text of either statute; nor could it. The California
 9 statute prohibits "knowingly access[ing] and without permission tak[ing], cop[ying], or mak[ing] use
 10 of any data" and "knowingly and without permission us[ing] or caus[ing] to be used computer
 11 services" (Cal. Penal Code § 502(c)(2), (3)); and the Nevada statute prohibits "knowingly, willfully
 12 and without authorization" engaging in certain actions to "a computer, system or network" or "data, a
 13 program or any supporting documents which exist inside or outside a computer" (Nev. Rev. Stat.
 14 § 205.4765(1), (3)). There is no prohibition in either statute on using automated download tools to
 15 access information from a website to which the user otherwise has access; indeed, the statutes do not
 16 in any way speak to the *means* of accessing or using websites. Rimini could have paid one person to
 17 spend 1,000 hours to download support materials one file at a time; it could have paid 1,000 people to
 18 spend one hour each to do the same; or it could have paid one person to spend 100 hours to write and
 19 execute a computer program to download the same material. The access to the website and use of the
 20 data are the same in each scenario and the criminal consequences should not—indeed, cannot—
 21 differ. Oracle makes no effort to reconcile its contrary position with the statutory text or history.

22 Instead, Oracle argues that *United States v. Christensen*, 801 F.3d 970 (9th Cir. 2015),
 23 dictates a different result. Opp. at 18. But *Christensen* does not say anything about website terms of
 24 use, the means of accessing or using a website, or anything else relevant to this case beyond
 25 describing the statute's plain language (which Oracle ignores). *Christensen* involved "a widespread
 26 criminal enterprise" that included bribing police officers and telephone company employees to
 27 illegally wiretap and record private conversations. 801 F.3d at 980-82. The court concluded that the
 28 defendants had the intent to violate the California anti-hacking statute because, although they logged

1 into the police and telephone company databases “with a valid password,” they subsequently took,
2 copied, and used information without permission for illegal purposes. *Id.* at 994-95.

Citing one sentence from *Christensen* out of context, Oracle argues that Rimini violated the California statute because “Defendants knew they were not permitted to use their automated programs to access and take from Oracle’s systems.” Opp. at 18. But *Christensen* did not hold (or even suggest) that any use of automated programs was unlawful. To the contrary, the opinion makes clear that “without permission” in the California statute modifies what a defendant does with the “information in the database,” and not the *means* a defendant uses to *access* the database. *Christensen*, 801 F.3d at 994; Cal. Penal Code § 502. Oracle never argued—nor could it—that Rimini violated the statute because of the way it *used* the data it downloaded; for this reason, *Christensen* establishes, if anything, that Rimini did not violate the California statute. Mot. at 17.

12 Oracle also argues in a footnote, citing *Nosal*, that a party can authorize certain methods of
13 access but not others. Opp. at 19 n.16. But Oracle quotes an example that the court in *Nosal*
14 explained was an *overbroad* and *impermissible* interpretation of the federal statute. 676 F.3d at 858
15 (stating, immediately after the language Oracle quotes, “[w]hile the CFAA is susceptible to the
16 government’s broad interpretation, we find *Nosal*’s narrower one more plausible”). Oracle’s reliance
17 on an example the Ninth Circuit specifically **rejected** makes clear that Rimini’s conduct here is
18 precisely what the Ninth Circuit expressly excluded from the scope of the federal statute.

At bottom, there is a difference between access and *means* of access that Oracle misses entirely. To the extent Oracle through its terms of use put restrictions on the means of accessing a website, such restrictions are purely contractual; so long as the access and use itself remains authorized, the anti-hacking statutes have no role to play. Nothing in the statutes purports to empower Oracle to create criminal offenses through private restrictions on means of access in its terms of use.

(ii) The statutes do not prohibit conduct simply because it violates a website terms of use

Oracle argues that Rimini acted “without permission” because the website terms of use did not permit the use of downloading tools. *E.g.*, Opp. at 20 (“Oracle’s authorization is determinative”

1 because “Oracle’s systems are at issue”). Yet, Oracle does not even *cite*, let alone address, the
 2 statutes or the relevant legislative history. Oracle offers no statutory interpretation of the terms
 3 “permission” or “authorization” that would extend to any violation of website terms of use. Nor does
 4 Oracle address the rule of lenity or the canon of constitutional avoidance. Instead, Oracle clings to its
 5 argument that because its website terms of use prohibited automated downloading tools, Rimini’s use
 6 of those tools amounts to unlawful computer hacking.

7 The Ninth Circuit has rejected a closely analogous argument. *See LVRC Holdings LLC v.*
Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009) (“No language in the CFAA supports [plaintiff’s]
 8 argument that authorization to use a computer ceases when an employee resolves to use the computer
 9 contrary to the employer’s interest”). And the Ninth Circuit in *Nosal* expressly rejected computer
 10 hacking liability based on a violation of terms of use. 676 F.3d at 860. Both cases reiterated that
 11 anti-hacking statutes must “be construed strictly.” *Nosal*, 676 F.3d at 863; *Brekka*, 581 F.3d at 1134.
 12 Oracle halfheartedly suggests the cases “involved the federal CFAA, not the state statutes at issue
 13 here.” Opp. at 19. But, as Rimini explained (Mot. at 22), the due process concerns that compelled
 14 the statutory interpretation in both cases apply equally to the similar state laws and require a similar
 15 statutory analysis. Oracle offers no reason why the state statutes can or should be read differently
 16 than the federal statute for purposes of constitutional avoidance.

17 According to Oracle, the Ninth Circuit held in *Brekka* that “LVRC’s authorization, not a third
 18 party’s, was determinative.” Opp. at 19-20. But there was *no third party involved* in *Brekka*—the
 19 case involved an employee using his employer’s computer. 581 F.3d at 1133. The salient fact in
Brekka was the employee’s “permission” to use the computer. *Id.* at 1135. As the court explained, a
 20 person lacks “authorization” “when the person *has not received permission* to use the computer for
 21 *any purpose.*” *Id.* (emphases added). Similarly, in *Nosal*, the court found no statutory violation
 22 “[b]ecause [the defendant’s] accomplices had permission to access the company database.” 676 F.3d
 23 at 864. Contrary to Oracle’s argument, the determinative fact was not that the *employer gave*
 24 permission (Opp. at 20), but that the “*accomplices had permission.*” *Nosal*, 676 F.3d at 864.

25 The Ninth Circuit’s reasoning is consistent with the plain language of the state statutes. The
 26 statutes address whether an individual acted with “permission” or “authorization,” not whether the
 27

1 owner of the computer gave permission. *See* Cal. Penal Code § 502(c); Nev. Rev. Stat. § 205.4765.
 2 Indeed, the Third Circuit, addressing the California anti-hacking statute, reversed and remanded
 3 because the district court erroneously “premised” its decision “on ownership of the server, and did
 4 not address whether [the defendant] had authorization or permission to access the server.” *Joseph*
 5 *Oat Holdings, Inc. v. RCM Digesters, Inc.*, 409 F. App’x 498, 505 (3d Cir. 2010). The court
 6 reasoned that “ownership of the server may be an important factor,” but “may not be determinative
 7 with respect to whether [the defendant] had permission to access the server.” *Id.*

8 Oracle relies on the jury instruction precluding liability if Rimini “believed it had
 9 authorization.” Opp. at 20, 24. While a good-faith belief is one defense under the statutes, it does
 10 not resolve the question whether Rimini acted with “permission.” Rimini requested a *separate*
 11 instruction related to “permission” that would have informed the jury that a client’s permission was
 12 sufficient in order to “explain[] the scope of the statute to the jury and prevent[] it from applying this
 13 vague and overbroad statute in a constitutionally impermissible way.” Dkt. 869 at 98-99. Oracle
 14 objected to that instruction (10/5 Tr. 3273:7-21), and the Court declined to so instruct the jury (Dkt.
 15 880 at 58). Oracle took advantage of that gap in the instructions by telling the jury in closing: “I told
 16 you about that when I went through the jury instructions. It’s not the clients authorizing it. It’s did
 17 Oracle authorize you to come on the computer. Answer, no.” 10/6 Tr. 3629:8-11.

18 The instructions actually given demonstrate that the jury’s liability verdict includes an
 19 implicit finding only that Rimini did not believe it had *Oracle’s* authorization—i.e., the jury found
 20 that Rimini knew it was violating the *website terms of use* when it used automated tools, which is *all*
 21 that Oracle argues even now. Opp. at 4 (Rimini “kn[ew] the Terms of Use prohibited [its] conduct”).
 22 But that verdict does not demonstrate that the jury found that Rimini knew it was committing
 23 *criminal computer hacking*, particularly under Oracle’s abusive and expansive reading of the statutes
 24 that courts have rejected. There is *no evidence* that Rimini knew it was violating anti-hacking
 25 statutes (and Oracle cites none), and the finding regarding Rimini’s belief does not support liability
 26 for criminal hacking under either statute. The problem with application of the anti-hacking statutes is
 27 a *legal* one, not a *factual* one: The conduct established at trial, viewed in the light most favorable to
 28 Oracle, demonstrates that the statutes are inapplicable to Rimini’s conduct as a matter of law.

1 Oracle had a remedy at law for the conduct for which it complains: a claim for breach of
 2 contract for violation of its website terms of use. Oracle initially pursued that remedy by alleging and
 3 pursuing the breach claim, but then abandoned the claim before sending the case to the jury. Dkt.
 4 852 at 2. Oracle continues to stress the contractual nature of the duty it claims Rimini breached,
 5 contending that Rimini “knew that [its] use of automated tools violated the Terms of Use” and “made
 6 a calculated decision to violate” the “Terms of Use,” attaching the contracts to its brief to support its
 7 arguments, and arguing that the choice-of-law clause in the contracts controls on the question of
 8 which state law applies. Opp. at 3-4, 12-13, 25; Dkt. 957-1. Indeed, Oracle does not identify a single
 9 difference between its breach of contract claim and its computer hacking claims. But Oracle’s
 10 attempt to substitute criminal anti-hacking offenses for the straightforward breach-of-contract claim it
 11 abandoned is like using a monkey wrench to adjust a watch spring—it is the wrong tool for the job.

12 Rimini explained that Oracle’s attempt to transform a breach of website terms of use into
 13 computer hacking would impermissibly displace settled commercial law and criminalize private and
 14 commercial behavior. Mot. at 16-17 (providing examples). For example, signing in to check a
 15 husband’s email at his request but contrary to Gmail terms of use would be criminal; posting through
 16 Facebook on a girlfriend’s page at her request but contrary to Facebook terms of use would be
 17 criminal; and using a third-year law student friend’s Westlaw password with her permission to pull a
 18 Law Review article would be criminal. The Ninth Circuit in *Nosal* also identified many similar
 19 examples. 676 F.3d at 858-62.

20 Oracle does not respond to these fundamental problems with its interpretation of the statutes,
 21 and implicitly acknowledges that this conduct would in fact be criminal under Oracle’s proposed
 22 interpretation of the state anti-hacking laws. Yet the Ninth Circuit has held on multiple occasions
 23 that the anti-hacking statutes must be read narrowly so as to keep the “focus on hacking rather than
 24 turning [the statute] into a sweeping Internet-policing mandate” that “would make criminals of large
 25 groups of people.” *Id.* at 858-59. The contrary view urged by Oracle would improperly turn
 26 “millions of unsuspecting individuals” into criminals and must be rejected. *Id.* at 859; *accord Valle*,
 27 807 F.3d at 527; *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 207 (4th Cir. 2012).

28 Oracle argues that breach of website terms of use can amount to computer hacking by citing a

1 2004 case from the Northern District of Texas. Opp. at 21. As the en banc Ninth Circuit has
 2 explained, outdated decisions like that “failed to consider the effect on millions of ordinary citizens”
 3 of an expansive reading and “failed to apply the long-standing principle that we must construe
 4 ambiguous criminal statutes narrowly.” *Nosal*, 676 F.3d at 862-63 (rejecting Fifth Circuit’s
 5 interpretation of federal anti-hacking statute). Since *Nosal* was decided, the two circuits to have
 6 considered the issue have agreed with *Nosal* that a narrow construction is necessary. *See Valle*, 807
 7 F.3d at 527; *Miller*, 687 F.3d at 206 (agreeing with *Nosal*, applying rule of lenity, and rejecting an
 8 interpretation that “has far-reaching effects unintended by Congress”).

9 Oracle also argues that Rimini relies “on the proposition that authorization under the CDAFA
 10 and NCCL can be defined by contract.” Opp. at 22. That is false. Under the rule of lenity, any legal
 11 authorization is sufficient (*Brekka*, 581 F.3d at 1135), and Rimini’s contracts with its clients
 12 undisputedly granted it permission to access the websites—permission that Oracle recognized could
 13 be granted to third parties (e.g., 9/22 Tr. 1107:15-19, 1201:10-13; PTX 1569). Such authorization
 14 could have come in different forms; here, it was through contracts.

15 Oracle’s final assertion is that it “made Defendants aware that their activities were
 16 impermissible.” Opp. at 22. In other words, Oracle gave notice that it thought Rimini was breaching
 17 the website terms of use. That does not solve the problem of turning a breach into a crime.

18 In short, the jury’s findings of liability under the California and Nevada anti-hacking statutes
 19 cannot be sustained. Oracle asserts the statutes were violated, but never addresses the text of the
 20 statutes, the directly relevant case law, or the governing canons of statutory construction. The Court
 21 can safely disregard such unfounded arguments. The undisputed facts applied to the statutes cannot
 22 support liability as a matter of law.

23 **2. The Statutory Provisions, Particularly as Oracle Seeks to Apply Them, Are
 24 Unconstitutional**

25 Even if Oracle were correct that the California or Nevada statutes cover Rimini’s use of
 26 automated download tools, judgment must nonetheless be entered for Rimini because applying the
 27 statutes to that conduct would be unconstitutional.

1 **a. The California and Nevada Statutes Are Unconstitutional as Applied to**
 2 **Rimini's Use of Automated Download Tools**

3 The Due Process Clause does not permit Oracle to unilaterally determine what constitutes
 4 criminal conduct in the state of California by drafting website terms of use and revising them at any
 5 time. *Nosal*, 676 F.3d at 862. Rimini explained this at length in its motion (Mot. at 21-22), but
 6 Oracle simply ignores that discussion.

7 Oracle dismisses *Nosal* by stating that “none of those concerns apply to Defendants.” Opp. at
 8 25. But Oracle’s focus on the allegedly “culpable behavior of the defendants” is inadequate because
 9 it “fail[s] to consider the effect on millions of ordinary citizens.” *Nosal*, 676 F.3d at 862. Indeed, the
 10 Second Circuit recently agreed with *Nosal*, applied the rule of lenity, and held that “we must construe
 11 the statute knowing that our interpretation … will govern many other situations.” *Valle*, 807 F.3d at
 12 528. The court *rejected* the very position Oracle asserts here. *See id.* (“disagree[ing]” with position
 13 that “concerns about the rule of lenity or about the risk of criminalizing ordinary behavior inherent in
 14 its broad construction” were not implicated when interpreting an anti-hacking statute). The Fourth
 15 Circuit also agreed with *Nosal*, refusing to “transform[] a statute meant to target hackers into a
 16 vehicle for imputing liability to [individuals] … who disregard a use policy” because “other legal
 17 remedies exist for these grievances” and it “is violative of the Supreme Court’s counsel to construe
 18 criminal statutes strictly.” *Miller*, 687 F.3d at 207.

19 Nor does it matter, as Oracle states, that “Ravin … and others actually knew about the Terms
 20 of Use … and made a calculated decision to violate them anyway.” Opp. at 25. Under *Nosal*, that is
 21 a breach of contract, not a violation of the anti-hacking statutes. The cease-and-desist letters that
 22 Oracle sent and its decision to block Rimini’s IP address were attempts by Oracle to enforce its
 23 website terms of use. But efforts to enforce website terms of use do not mitigate the constitutional
 24 problems inherent in transforming even an intentional violation of those terms into a criminal act.
 25 *See Nosal*, 676 F.3d at 860. As the court in *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009),
 26 explained: “[I]f any conscious breach of a website’s terms of service is held to be sufficient by itself
 27 to constitute intentionally accessing a computer without authorization … the result will be that [the
 28 anti-hacking law] becomes a law that affords too much discretion to the police and too little notice to

1 citizens who wish to use the [Internet].” *Id.* at 467 (citation omitted). In short, notice of website
 2 terms of use is not the same as notice of criminal behavior, particularly when Oracle seeks to
 3 radically expand the reach of these laws well beyond the bounds recognized by the Ninth Circuit.

4 Oracle also misconstrues *Craigslist Inc. v. 3Taps Inc.*, 964 F. Supp. 2d 1178 (N.D. Cal. 2013),
 5 in arguing that “there are no serious constitutional doubts” because Rimini sought to avoid an IP
 6 address block. Opp. at 23. In *Craigslist*, the court “rejected” the position Oracle advocates here,
 7 holding that a violation of website terms of use does not constitute a claim under the federal anti-
 8 hacking statute. 964 F. Supp. at 1181 n.3. In considering a subsequent motion to dismiss regarding a
 9 “narrow statutory interpretation question,” the court overruled the defendant’s argument “that an
 10 owner of a publicly accessible website has no power to revoke the authorization of a specific user to
 11 access that website.” *Id.* at 1180. The “narrow” holding and specific facts of that case do not support
 12 Oracle’s extreme position here. The underlying problem, ignored by Oracle but emphasized in
 13 *Nosal*, is that contractual terms can change from day to day, but the criminal law does not. Here,
 14 Oracle permitted the use of automated download tools in 2006 and then prohibited them in 2007.
 15 Using those tools after they were eventually prohibited in 2007 may therefore be a breach of contract,
 16 but the conduct is no more criminal in 2007 than it was in 2006. Holding otherwise would vest the
 17 power to make criminal law in the hands of private parties, like Oracle, who can and will do so
 18 unilaterally and with no or insufficient notice. Such an interpretation is clearly unconstitutional. *See*
 19 *Nosal*, 676 F.3d at 860. This Court should, consistent with *Nosal* and *Valle*, apply the canon of
 20 constitutional avoidance to avoid this unconstitutional application of the statutes.

21 **b. The Statutory Provisions Are Unconstitutionally Void for Vagueness**

22 Although the Court need not reach this issue if it rules in Rimini’s favor on any of the
 23 preceding arguments, the statutory provisions are *also* unconstitutionally void for vagueness because
 24 they do not define the criminal offense with sufficient definiteness and because they allow for
 25 arbitrary enforcement. Mot. at 19-21.

26 Oracle’s short response, which does not address either prong of the void-for-vagueness
 27 standard, misconstrues two cases. In *People v. Hawkins*, 98 Cal. App. 4th 1428 (2002) (cited Opp. at
 28 23), the court considered a single and completely separate provision of the California statute and

1 ***expressly did not consider*** the provisions at issue here. *Id.* at 1441 (“What defendant claims is vague
 2 is not the above quoted definition of the crime, but the statute’s description of an exception or
 3 exemption from prosecution”). And the *Christensen* case does not even address the constitutionality
 4 of the California statute; it is therefore not relevant on that point. *E.g., United States v. Boeing Co.*, 9
 5 F.3d 743, 749 n.5 (9th Cir. 1993) (case not “authority” when it “did not squarely face the
 6 constitutional issues presented in [current] case”).³

7 Oracle claims that the “scienter requirements alleviate vagueness concerns.” Opp. at 24
 8 (citation omitted). But the offenses in the statutes are so limitless that a *mens rea* requirement does
 9 not provide individuals with adequate notice that they are committing a crime. *E.g., Drew*, 259
 10 F.R.D. at 467 (rejecting the argument Oracle makes, explaining the scienter requirement is “basically
 11 eliminate[d]” by Oracle’s position “that the ‘intentional’ requirement is met simply by a conscious
 12 violation of a website’s terms of service” because “there is absolutely no limitation or criteria as to
 13 which of the breaches should merit criminal prosecution”). Indeed, in all of the examples cited in
 14 Rimini’s motion (Mot. at 20), the individuals would have acted intentionally, but, much to their
 15 surprise, illegally. Oracle fails to address these examples.

16 **3. The State Law Hacking Claims Fail for Additional Reasons**

17 Oracle International Corporation lacks standing and the record does not support application of
 18 California law to Oracle’s claims.

19 **a. Oracle International Corporation Lacks Standing**

20 The jury awarded damages to two Oracle entities for Rimini’s purported violation of the anti-
 21 hacking statutes—Oracle International Corporation (\$5.6 million) and Oracle America, Inc. (\$8.827
 22 million). Oracle America provides support services, and Oracle International Corporation does not.
 23 It is undisputed that Rimini did not access or use data from any computer systems owned by Oracle
 24 International Corporation. *E.g.*, 9/24 Tr. 1772:18-1773:3. Under the plain language of the statutes,

25 ³ Oracle’s opening sentence—that Rimini “never moved to dismiss” the hacking claims (Opp.
 26 at 23)—is wrong twice over. Rimini moved to dismiss Oracle’s computer hacking claims on *two*
 27 occasions. Dkt. 29 at 2-10; Dkt. 48 at 2-7. And Rimini does not request that the Court “hold
 28 these statutes entirely unconstitutional” (Opp. at 23)—rather, Rimini’s arguments are targeted
 specifically at “[t]he four provisions at issue” under which the jury found liability, *not* the rest of
 the lengthy statutes. Mot. at 19 (emphasis added).

1 Oracle International Corporation lacks standing to pursue the claims, and the verdict must therefore
 2 be reduced by the \$5.6 million awarded to Oracle International Corporation. Mot. at 9.

3 Oracle argues that “licensing revenue” gives it an “interest in the data.” Opp. at 16 & n.13.
 4 But the California statute requires that a party be an “*owner or lessee*” of the data to have standing,
 5 which Oracle International Corporation undisputedly is not; the statute says nothing about an
 6 “interest” in the data. Cal. Penal Code § 502(e)(1) (emphasis added). Indeed, in each case Oracle
 7 cites, the plaintiff *owned* the data at issue. As for the Nevada statute, Oracle has offered no basis
 8 upon which Oracle International Corporation is a “victim” under the statute, as required. Supposed
 9 lost profits *cannot* create standing under the statute. *See infra* Section II.B.1.⁴

10 **b. The Record Does Not Support Application of the California Statute**

11 Where, as here, the record does not identify where the conduct occurred, or where the affected
 12 servers were located, then the Commerce Clause and choice-of-law principles render the claim
 13 legally unsupportable as a matter of law. Mot. at 9-12.

14 Oracle asserts that *any* state’s law can be applied so long as it does not “conflict with the
 15 public policy of the forum state.” Opp. at 11 (citation omitted). Yet Oracle could not, for example,
 16 march into court and assert a Vermont state law claim against Rimini absent a substantial nexus to
 17 Vermont. *E.g., Ferdie Sievers & Lake Tahoe Land Co. v. Diversified Mortg. Inv.*, 95 Nev. 811, 816
 18 (1979) (Nevada law did not apply to transaction “having little or no relation to anything done or to be
 19 done within Nevada” as compared to prior case where Nevada law applied when “transaction … was
 20 wholly within this state”). The issue is not the Full Faith and Credit Clause as Oracle misdirects
 21 (Opp. at 11), but the lack of evidence supporting a *nexus* to California. Oracle points out that it is
 22 headquartered in California and that one instance of automated downloading occurred in northern
 23 California. Opp. at 12. But it does not dispute that the conduct could have involved a Kansas client’s
 24 ID to access an Oracle server in Texas, or that the rest of the conduct could have happened outside of
 25 California—all facts that would (Oracle does not dispute) preclude application of California law.

26
 27 ⁴ Rimini did not waive this standing argument, as Oracle contends. Rimini’s Rule 50(a) motion
 28 section relating to *all* of Oracle’s computer claims argued that “Oracle International Corporation
 failed to prove it even had computer systems” (Dkt. 838 at 13 n.3), and nothing more is required.

1 E.g., *Healy v. Beer Institute*, 491 U.S. 324, 335-36 (1989); *GMC v. Eighth Judicial Dist. Court of*
 2 *Nev.*, 122 Nev. 466, 478 (2006).

3 The problem is one that Oracle recognizes: a state cannot “attempt[] to reach ‘wholly’ out of
 4 state commerce.” Opp. at 15. California laws are presumptively not applied extraterritorially, as the
 5 California Supreme Court observed in a case in which Oracle Corporation successfully sought to
 6 prevent the application of California labor laws to its out-of-state employees. *Sullivan v. Oracle*
 7 *Corp.*, 51 Cal. 4th 1191, 1207 (2011). Nor does the choice-of-law agreement resolve the issue (Opp.
 8 at 12-13) because it is not part of the trial record, and in any event because parties cannot agree to
 9 application of a statute absent a nexus supporting application of that state’s law. Cf. *Gravquick A/S v.*
 10 *Trimble Navigation Int’l*, 323 F.3d 1219, 1224 (9th Cir. 2003) (dormant commerce clause not
 11 violated when there were “sufficient connections with California to support a California choice of
 12 law”); *Ferdie*, 95 Nev. at 817 (parties can stipulate to application of “laws of a state to which the
 13 transaction has a substantial nexus”).⁵

14 B. Lost Profits Are Unavailable for Oracle’s State Law Hacking Claims

15 Lost profits are not an available remedy for a violation of either the California or Nevada anti-
 16 hacking statutes, and Oracle still has not identified a single customer that left Oracle because of the
 17 automated downloading that occurred over a three-month period. As a result, the \$14.4 million lost
 18 profits award must be vacated, even if Rimini is liable under either or both statutes.

19 1. Lost Profits Are Not Recoverable Under the Statutes

20 Oracle essentially ignores Rimini’s extensive statutory and legislative history analysis

21
 22 ⁵ Oracle’s claim that Rimini waived this argument fails because Rimini’s repeated broad assertions
 23 regarding the failures of Oracle’s ever-changing computer hacking claims are sufficient to
 24 preserve the more specific argument. See, e.g., Dkt. 29 (Mot. to Dismiss), 739 (Trial Br.), 766
 25 (Jury Instruction Br.), 838 (Rule 50(a) Mot.). Indeed, the Ninth Circuit explained in *E.E.O.C. v.*
 26 *Go Daddy Software, Inc.*, 581 F.3d 951, 960 (9th Cir. 2009) (cited Opp. at 9 n.3), that an
 27 “ambiguous” Rule 50(a) motion is sufficient to preserve more specific arguments. Oracle relies
 28 on inapposite cases in which no Rule 50(a) motion was filed (*Freund v. Nycomed Amersham*, 347
 F.3d 752, 761 (9th Cir. 2003)), and where the district court entered judgment as a matter of law
 “on grounds not asserted in [the] party’s motion for directed verdict” (*Murphy v. City of Long*
Beach, 914 F.2d 183, 186 (9th Cir. 1990)). Further, purely legal arguments are not waived absent
 unfair surprise, which Oracle has not demonstrated, and the Ninth Circuit has gone so far as to
 resolve Commerce Clause arguments not even raised in the district court at all. See *Abramson v.*
Brownstein, 897 F.2d 389, 391 (9th Cir. 1990).

1 explaining why lost profits are not recoverable under the California anti-hacking statute. *Compare*
 2 Opp. at 26, *with* Mot. at 23-25. Instead, Oracle relies on the generic proposition that “[u]nder
 3 California law, ‘compensatory damages’ include ‘lost profits.’” Opp. at 26. Oracle cites just two
 4 cases for this proposition (*Sanchez-Corea v. Bank of America*, 38 Cal. 3d 891, 906-07 (1985), and
 5 *Elec. Funds Solutions v. Murphy*, 134 Cal. App. 4th 1161, 1179-80 (2005)), but neither case has
 6 anything to do with the California anti-hacking statute, and neither case analyzes the term
 7 “compensatory damages” as a matter of statutory interpretation. Oracle also relies on *Capitol Audio*
 8 *Access, Inc. v. Umemoto*, 980 F. Supp. 2d 1154 (E.D. Cal. 2013), but the court in that case did not
 9 hold or even imply that lost profits were recoverable under the California statute.⁶

10 Oracle has nothing to say about the Nevada law except to state without explanation or citation
 11 that “[d]amages for ‘loss’ or ‘injury’ plainly include lost profits, at least.” Opp. at 27. Yet, as Rimini
 12 explained, the plain language of the statute “limits damages to investigation costs *and* damages that
 13 are directly attributable to ‘the crime.’” Mot. at 25 (emphasis added). Federal courts, interpreting
 14 analogous language in the federal anti-hacking statute, have held that lost profits are too far removed
 15 from the harm that the statutes protect against to be recoverable. *E.g.*, *Farmers Ins. Exchange v.*
 16 *Steele Ins. Agency, Inc.*, 2013 U.S. Dist. LEXIS 104606, at *59 (E.D. Cal. July 25, 2013).

17 Oracle dismisses the federal cases on the basis that “‘loss’ is a defined term in the CFAA that
 18 relates to standing.” Opp. at 27. Oracle is wrong. The federal statute, like the Nevada statute, allows
 19 a plaintiff to recover for “damage or loss.” 18 U.S.C. § 1030(g). It provides a definition of “loss”
 20 that is similar to the “response costs” and “loss” in the Nevada statute. *Compare* 18 U.S.C.
 21 § 1030(e)(1), *with* Nev. Rev. Stat. §§ 205.4759, 205.511. And the Ninth Circuit explained for the
 22 federal anti-hacking law, consistent with subsequent district court decisions, that “[d]amages are
 23 indeed limited to those caused by the impairment, which may not be the same thing as the expenses

24

25 ⁶ Oracle “objects” to the legislative history because “[t]here is no ambiguity” in the text of either
 26 statute. Opp. at 23 n.18; *id.* 27 n.21 (same). Oracle is wrong again. The lengthy statutes are full
 27 of terms that courts have found ambiguous in similar circumstances, such as “permission,”
 “authorization,” “computer services,” and “supporting documents.” *E.g.*, *Brekka*, 581 F.3d at
 28 1134-35 (applying rule of lenity to interpret ambiguous term “authorization”); *Drew*, 259 F.R.D.
 (describing a wide variety of judicial interpretations of different terms in the federal
 anti-hacking statute).

1 of the victim subsequent to the impairment.” *Creative Computing v. Getloaded.com LLC*, 386 F.3d
 2 930, 936 (9th Cir. 2004). Thus, the federal cases are highly instructive, particularly in the absence of
 3 any cases interpreting the similar Nevada statute.

4 In short, the state statutes address computer hacking and contemplate the recovery of only
 5 those damages that are directly associated with the impairment or destruction of computer services or
 6 data. The statutes do not, however, create a right to seek remote and speculative damages far
 7 attenuated from actual impairment, such as lost profits. Oracle is thus asking this Court to be the first
 8 anywhere to approve such a recovery, yet offers no statutory or decisional support for that request.
 9 That is a tacit admission that \$14.4 million of the jury’s award cannot be sustained as a matter of law.

10 **2. There Is No Evidence Supporting an Award of Lost Profits**

11 Even if lost profits were an available remedy under the state statutes, the record in this case
 12 contains legally insufficient evidence to support the jury’s \$14.4 million award of lost profits for
 13 three months of unrelated and sporadic activity. Mot. at 26-27. Indeed, Oracle does not identify a
 14 single customer it lost as a result of Rimini’s automated downloading. That award cannot stand.

15 Instead, Oracle’s tortured reasoning is that “Rimini’s clients ‘need’ a library of support
 16 materials” and that “Rimini was under intense time pressure to complete the download before its new
 17 customers’ Oracle maintenance end dates,” and therefore Rimini’s actions apparently *caused* those
 18 clients to leave Oracle. Opp. at 27-28. But there is a fatal flaw in this made-up theory—it does not
 19 explain how *Oracle* lost profits. As Oracle acknowledges, the clients at issue *already* had
 20 maintenance *end* dates, which means *they had already decided to leave Oracle*.

21 Oracle bore the burden of proving that these customers *would have* stayed with Oracle, but
 22 after a full trial on the merits, the evidentiary record is clear that Oracle did not, because it could not,
 23 meet that burden. Nor does Oracle dispute that its experts failed to identify a single customer who
 24 left Oracle *because of* Rimini’s use of automated tools. Entirely absent from the record is any
 25 evidence that, for example, Rimini represented to potential clients that its automated download tools
 26 were far superior to clicking manually through Oracle’s database, such that clients made the decision
 27 to leave Oracle and join Rimini. The absence of this causal link is fatal to any award of lost profits.
 28 Rimini made this point clearly in its motion (Mot. at 27), and Oracle has not disputed it.

1 Oracle also does not dispute that its theory of lost profits was a subset of its copyright lost
 2 profits analysis. It recognizes that Ms. Dean calculated “lost profits from the loss of the customers
 3 whose logins were used.” Opp. at 7. As Ms. Dean confirmed at trial, she took the “customer IDs
 4 [that] were ultimately used” for automated downloading, and looked up those customers in her
 5 *copyright* “lost profits calculations.” 9/24 Tr. 1832:21-1833:19. “[I]n the instance that [she] was
 6 *already claiming* [copyright] lost profits for” those customers, she “add[ed] up” those copyright lost
 7 profits and presented them as computer hacking lost profits. *Id.* (emphasis added). But if “they
 8 [were] not in the [copyright] lost profits,” she “didn’t add anything.” *Id.* Beyond tallying clients off
 9 her copyright list, she did not testify to engaging in any independent lost profits analysis specific to
 10 computer hacking. *E.g., id.* Ms. Dean’s testimony therefore does not provide actual *evidence* of lost
 11 profits *caused by* computer hacking. To the contrary, her theory of computer hacking lost profits—
 12 which was not even disclosed in her expert report—is speculative and nonsensical because Oracle has
 13 not established any connection between copyright and computer hacking lost profits that would
 14 support simply switching lost profits from one category to another.

15 Oracle highlights this failure when it states with no reasoning that “[t]he jury was entitled to
 16 infer that computer abuse caused these losses, even if the evidence did not support a quantification of
 17 copyright lost profits.” Opp. at 28. Just the opposite: The only evidence Oracle attempted to present
 18 at trial was *copyright* lost profits (for which the jury found \$0 of lost profits), and there was *no*
 19 *evidence*—and Oracle identifies none—showing Oracle lost profits *because of* computer hacking.
 20 The jury is not entitled to infer something for which no evidence exists, and Ms. Dean’s hollow
 21 testimony cannot support an award of computer hacking lost profits.

22 Finally, Oracle contends that the jury’s award of copyright lost profits for hacking claims is
 23 not duplicative or preempted because the anti-hacking statutes “contain extra elements … and protect
 24 qualitatively different rights,” and because the jury was instructed to award non-duplicative damages.
 25 Opp. at 28-29. The preemption problem is that Oracle seeks to recover *copyright damages* through a
 26 state law cause of action. That leads to a specific type of preemption not addressed in Oracle’s
 27 generic cases. *Compare* Opp. at 28, *with* Mot. at 27 n.10. And the damages were duplicative
 28 because, apart from the \$27,000 of investigation costs, they were *copyright* damages. 9/24 Tr.

1 1832:21-1833:19. Oracle also asserts that Oracle America was not compensated for copyright
 2 infringement at the same time it inconsistently defends its assertion that Oracle International
 3 Corporation can recover for computer hacking. Opp. at 28.

4 Oracle also spends a page describing “[h]arm [t]o Oracle’s [s]ystems” (Opp. at 6-7), but does
 5 not dispute that it never quantified or sought damages for slowdowns or for the one system reboot.
 6 Oracle had every opportunity at trial to identify and quantify harm it allegedly suffered, but the
 7 undisputed evidence shows that Oracle suffered only \$27,000 in investigation costs. No evidence
 8 supports even one cent of the \$14.4 million of lost profit damages, and therefore even if lost profits
 9 were an available remedy, the award must be vacated here. At most, only \$27,000 can be awarded on
 10 the state anti-hacking claims.

11 **C. Oracle Concedes Judgment Is Warranted on Its Other Claims**

12 Oracle does not respond to, and therefore concedes, Rimini’s argument that Oracle has
 13 abandoned its claims for unfair practices and an accounting. Mot. at 28 n.13. Judgment is therefore
 14 warranted on those claims. Oracle also acknowledges that judgment is warranted on its separate
 15 equitable restitution claim because it “seeks only a UCL judgment of liability and injunctive relief.”
 16 Opp. at 15 n.10. And Oracle agrees that its UCL claims “fail together” with its California hacking
 17 claim. *Id.* The Court should therefore enter judgment against Oracle on *all* of its state law claims—
 18 which stands to reason, because this is and always has been a case involving allegations of copyright
 19 infringement.

20 **III. CONCLUSION**

21 For the foregoing reasons, Rimini respectfully requests that the Court enter judgment on
 22 Oracle’s California and Nevada computer hacking claims, California Unfair Competition Law claim,
 23 unfair practices claim, equitable restitution, and an accounting.

25 DATED: January 8, 2016

GIBSON, DUNN & CRUTCHER LLP

26 By: s/ Blaine H. Evanson
 27 Blaine H. Evanson

28 *Attorneys for Defendants
 Rimini Street, Inc. and Seth Ravin*

CERTIFICATE OF SERVICE

I hereby certify that on January 8, 2016, I caused to be electronically filed the foregoing document with the clerk of the court for the U.S. District Court, District of Nevada, using the electronic case filing system. The electronic case filing system sent a "Notice of Electronic Filing" to the attorneys of record who have consented in writing to accept this Notice as service of this document by electronic means.

By: s/ Blaine H. Evanson
Blaine H. Evanson

*Attorney for Defendants
Rimini Street, Inc. and Seth Ravin*